CVE-2003-0047

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2003-0047
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-02-19 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	SSH2 clients for VanDyke (1) SecureCRT 4.0.2 and 3.4.7, (2) SecureFX 2.1.2 and 2.0.4, and (3) Entunnel 1.0.2 and earlier

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Van Dyke Technologies	Entunnel	All	All	All	All

Application	Van Dyke Technologies	Securecrt	3.4.7	All	All	All
Application	Van Dyke Technologies	Securecrt	4.0.2	All	All	All
Application	Van Dyke Technologies	Securefx	2.0.4	All	All	All
Application	Van Dyke Technologies	Securefx	2.1.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	So
iDEFENSE	af
VanDyke Entunnel SSH2 Client Software Access Control Bug May Disclose Passwords to Local Users Via Memory - SecurityTracker	af
Van Dyke SecureCRT SSH2 Authentication Password Persistence Weakness	af
VanDyke SecureFX SSH2 Client Software Access Control Bug May Disclose Passwords to Local Users Via Memory - SecurityTracker	af
marc.info	af
Van Dyke Software Entunnel SSH2 Authentication Password Persistence Weakness	af
Van Dyke Software SecureFX SSH2 Authentication Password Persistence Weakness	af
VanDyke SecureCRT SSH2 Client Software Access Control Bug May Disclose Passwords to Local Users Via Memory - SecurityTracker	af
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.